CLAIM AMENDMENTS

1   1.   (Currently Amended) A method for facilitating Internet security protocol (IPsec)

2   based communications through a device that employs address translation in a

3   telecommunications network, the method comprising the steps of:

4   receiving a first electronic message from a first node, wherein:

5   the first node is associated with a first network address;

6   the first electronic message is based on IPsec; and

7   the first electronic message is associated with a first identifier;

8   the first identifier is generated by the first node; and

9   the first electronic message is addressed to a second network address;

10   the device generating a value based on the first identifier and a specified scheme;

11   sending the first electronic message to a second node based on the second network

12   address, wherein the first electronic message includes a particular network

13   address that is associated with the device instead of the first network address;

14   receiving a second electronic message from the second node, wherein:

15   the second electronic message is based on IPsec; and

16   the second electronic message is addressed to the particular network address;

17   the second electronic message is associated with a second identifier that is

18   different than the first identifier;[[,]] wherein and

19   the second identifier is generated, based on the first identifier and the specified

20   scheme, by the second node;

21   the device determining whether the second electronic message is directed to the first

22   node based on the value and the second identifier; and

23   sending the second electronic message to the first node at the first network address

24   when the second electronic message is determined to be directed to the first

25   node.

1   2.   (Currently Amended) A method as recited in claim 1, further comprising the steps of:

2   receiving a third electronic message from a third node, wherein:

3   the third node is associated with a third network address;

4   the third electronic message is based on IPsec; ~~and~~

5   the third electronic message is associated with a third identifier;

6   the third identifier is generated by the third node; and

7   the third electronic message is addressed to the second network address;

8   the device generating an additional value based on the third identifier and the

9   specified scheme;

10   sending the third electronic message to the second node based on the second network

11   address, wherein the first electronic message includes the particular network

12   address that is associated with the device instead of the third network address;

13   ~~wherein the step of receiving comprises~~

14   receiving, after sending the first electronic message and the third electronic message

15   to the second node, the second electronic message from the second node[[,]];

16   wherein:

17   the second electronic message is based on IPsec; ~~and~~

18   the second electronic message is addressed to the third network address;

19   the second electronic message is associated with the second identifier that is

20   different than the first identifier and the third identifier; and

21   the second identifier is generated, based on the third identifier and the

22   specified scheme, by the second node;

23   the device determining whether the second electronic message is directed to the third

24   node based on the additional value and the second identifier; and

25   when the second electronic message is determined to be directed to the third node,

26   sending the second electronic message to the third node at the third network

27   address.

1   3.   (Cancelled)

1   4.   (Currently Amended) A method as recited in claim 3 1, wherein the specified scheme

2   is selected from the group consisting of a first scheme that produces a fixed length

3   output, a second scheme that includes a hash algorithm, and a third scheme that

4   includes a Message Digest 5 one-way hash function.

1   5.   (Cancelled)

1   6.   (Cancelled)

1   7.   (Cancelled)

1   8.   (Cancelled)

1   9.   (Currently Amended) A method as recited in claim 8 1, wherein:

2   the value is a hash value;

3   the second identifier is based at least in part on the hash value;

4   the hash value is comprised of a first plurality of bytes;[[,]] wherein

5   the second identifier is comprised of a second plurality of bytes;[[,]] and wherein

6   a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first

7   plurality of bytes;[[,]] and wherein

8   the step of determining whether the second electronic message is directed to the first

9   node further comprises the step steps of:

10   comparing the last pair of bytes of the second identifier to the first pair of

11   bytes of the hash value; and

12   when the last pair of bytes of the second identifier match the firs pair of bytes

13   of the hash value, determining that the second electronic message is

14   directed to the first node.

1   10.   (Currently Amended) A method as recited in claim 1, wherein:

2   the first node is an IPsec originator node;

3   the second node is an IPsec responder node;

4   the first identifier is a first IPsec security parameter index; and

5	the second identifier is a second IPsec security parameter index;
6	the device employs a feature selected from the group consisting of network address
7	translation (NAT), dynamic address NAT, and network address port
8	translation (NAPT);
9	and the method further comprises the steps of:
10	creating and storing a mapping between the value and the first IPsec security
11	parameter index;
12	creating an association between the value and the first identifier; and
13	storing the association in a translation table.

1	11.	(Currently Amended) A method as recited in claim 1, wherein the first electronic
2		message is based on IPsec tunnel mode and the second electronic message is are both
3		based on an IPsec feature selected from the group consisting of IPsec tunnel mode and
4		IPsec Encapsulation Security Payload.

1	12.	(Cancelled)

1	13.	(Cancelled)

1	14.	(Cancelled)

1	15.	(Cancelled)

1	16.	(Currently Amended) A method as recited in claim 1, further comprising the steps of:
2		when the second electronic message is determined to be directed to the first node,
3		creating an association between the first identifier network address and the
4		second identifier; and
5		storing the association in a table;
6		receiving a third electronic message from the second node, wherein the third
7		electronic message is based on IPsec and is associated with the second
8		identifier; and
9		determining that the third electronic message is directed to the first node based on the
10		association.

Docket No. 50325-0616 (Seq.No. 4621)

1   17.   (Cancelled)

1   18.   (Currently Amended) A method as recited in claim 1, further comprising the steps of:

2   receiving a third electronic from the second node, wherein:

3   the third electronic message is based on IPsec; and

4   the third electronic message is addressed to the specified network address;

5   the third electronic message is associated with a third identifier that is

6   different than both the first identifier and the second identifier;

7   the third identifier is generated, based on the first identifier and the specified

8   scheme, by the second node;

9   the device determining whether the third electronic message is directed to the first

10   node based on the value and the third identifier; and

11   when the third electronic message is determined to be directed to the first node,

12   sending the third electronic message to the first node at the first network

13   address.

1   19.   (Currently Amended) A method as recited in claim 1, wherein the step of the device

2   generating the value is performed before the step of receiving the second electronic

3   message.

1   20.   (Currently Amended) A method as recited in claim 1, wherein the step of the device

2   generating the value is performed after the step of receiving the second electronic

3   message.

1   21.   (Cancelled)

1   22.   (Cancelled)

1   23.   (Cancelled)

1 24. (Currently Amended) A method for facilitating Internet security protocol (IPsec)

2 based communications through a device that employs address translation in a

3 telecommunications network, the method comprising the steps of:

4 receiving a first electronic message from a first node, wherein:

5 the first node is associated with a first network address;

6 the first electronic message is based on IPsec; and

7 the first electronic message is associated with a first identifier[[,]]; wherein

8 the first identifier is generated by the first node based on a second identifier

9 and a specified scheme; and

10 the first identifier is different than the second identifier; and

11 the first electronic message is addressed to a second network address;

12 sending the first electronic message to a second node based on the second network

13 address, wherein the first electronic message includes a particular network

14 address that is associated with the device instead of the first network address;

15 receiving a second electronic message from the second node, wherein:

16 the second electronic message is based on IPsec; and

17 the second electronic message is address to the particular network address;

18 the second electronic message is associated with the second identifier; and

19 the second identifier is generated by the second node;

20 the device generating a value based on the second identifier and the specified scheme;

21 the device determining whether the second electronic message is directed to the first

22 node based on the value and the first identifier; and

23 sending the second electronic message to the first node at the first network address

24 when the second electronic message is determined to be directed to the first

25 node.

1 25. (Currently Amended) A method An apparatus for facilitating Internet security

2 protocol (IPsec) based communications with a device that employs address translation

3 in a telecommunications network, the method apparatus comprising the steps of:

4 a processor; and

5	one or more stored sequences of instructions which, when executed by the processor,
6	cause the processor to carry out the steps of:
7	generating a value based on <u>both</u> a first identifier that is associated with a first node
8	<u>and a specified scheme, wherein the first identifier is generated by the first</u>
9	<u>node;</u>
10	<u>the apparatus</u> generating a second identifier based on the value <u>and the specified scheme;</u>
11	receiving, from the device that employs address translation, a first electronic message
12	that originates from the first node, wherein<u>:</u>
13	the first electronic message is based on IPsec<u>;</u> ~~and~~
14	<u>the first electronic message</u> is associated with the first identifier;
15	<u>the first electronic message includes a particular network address that is</u>
16	<u>associated with the apparatus instead of a first network address that is</u>
17	<u>associated with the first node; and</u>
18	<u>the first electronic message is addressed to a second network address that is</u>
19	<u>associated with the second node;</u>
20	in response to receiving the first electronic message, generating a second electronic
21	message to the first node, wherein<u>:</u>
22	the second electronic message is based on IPsec<u>;</u> ~~and~~
23	<u>the second electronic message</u> is associated with the second identifier; <u>and</u>
24	<u>the second electronic message is addressed to the particular network address;</u>
25	sending the second electronic message to the device that employs address translation
26	<u>at the particular network address;</u>
27	wherein the device determines whether the second electronic message is directed to the
28	first node based on the second identifier and ~~an additional~~ <u>the</u> value <u>that is</u>
29	<u>generated by the device</u> based on the first identifier <u>and the specified scheme;</u> and
30	wherein the device sends the second electronic message to the first node <u>at the first</u>
31	<u>network address</u> when the device determines that the second electronic
32	message is directed to the first node.

1	26.	(Cancelled)

1   27.   (Cancelled)

1   28.   (Currently Amended) A method An apparatus as recited in claim 27 25, wherein the
2   value is a hash value, the first identifier is a first IPsec Security Parameter Index (SPI),
3   the second identifier is a second IPsec SPI, and the step of instructions for generating
4   the second IPsec SPI further comprises one or more stored sequences of instructions
5   which, when executed by the processor, cause the process to carry out the step of
6   generating, prior to receiving the first electronic message, the second IPsec SPI based
7   on the hash value.

1   29.   (Currently Amended) A method An apparatus as recited in claim 28 25, wherein the
2   value is a hash value, the first identifier is a first IPsec Security Parameter Index (SPI),
3   the second identifier is a second IPsec SPI, the first IPsec SPI is a first randomly
4   generated fixed length value and the step of instructions for generating the second
5   IPsec SPI further comprises one or more stored sequences of instructions which, when
6   executed by the processor, cause the process to carry out the step of generating the
7   second IPsec SPI based on at least a first portion of the hash value and a second
8   portion of a second randomly generated fixed length value.

1   30.   (Currently Amended) A method An apparatus for facilitating Internet security
2   protocol (IPsec) based communications through a router that employs network address
3   translation in a telecommunications network, the method apparatus comprising the
4   steps of:
5   a processor; and
6   one or more stored sequences of instructions which, when executed by the processor,
7   cause the processor to carry out the steps of:
8   receiving a first electronic message from a first IPsec originator node, wherein:
9   the first IPsec originator node is associated with a first network address;
10   the first electronic message is secured using IPsec: and
11   the first electronic message is associated with a first security parameter index
12   (SPI);

13   the first SPI is generated by the first IPsec originator node; and

14   the first electronic message is addressed to a third network address;

15   the router generating a first hash value based on the first SPI and a hash algorithm;

16   sending the first electronic message to an IPsec responder node based on the third

17   network address, wherein the first electronic message includes a particular

18   network address that is associated with the router instead of the first network

19   address;

20   receiving a second electronic message from a second IPsec originator node, wherein:

21   the second IPsec originator node is associated with a second network address;

22   the second electronic message is secured using IPsec; and

23   the second electronic message is associated with a second SPI;

24   the second SPI is generated by the second IPsec originator node; and

25   the second electronic message is address to the third network address;

26   the router generating a second hash value based on the second SPI and the hash

27   algorithm;

28   sending the second electronic message to the IPsec responder node based on the third

29   network address, wherein the second electronic message includes the

30   particular network address that is associated with the router instead of the

31   second network address;

32   after sending the first electronic message and the second electronic message to the

33   IPsec responder node, receiving a third electronic message from the IPsec

34   responder node, wherein:

35   the third electronic message is secured using IPsec; and

36   the third electronic message is associated with a third SPI that is different than

37   the first SPI and the second SPI[[,]]; wherein

38   the third electronic message is addressed to the particular network address;

39   the third SPI is generated by the IPsec responder node based at least in part on

40   the hash algorithm;

41   the router determining whether the third electronic message is directed to the first

42   IPsec originator node based on the first hash value and the third SPI;

43   when the third electronic message is determined to be directed to the first IPsec

44   originator node, sending the third electronic message to the first IPsec

45   originator node at the first network address;

46   determining whether the third electronic message is directed to the second IPsec

47   originator node based on the second hash value and the third SPI; and

48   when the third electronic message is determined to be directed to the second IPsec

49   originator node, sending the third electronic message to the second IPsec

50   originator node at the second network address.

1   31.   (Currently Amended) ~~A method~~ An apparatus as recited in claim 30, wherein the first

2   electronic message is based on IPsec tunnel mode and IPsec Encapsulating Security

3   Payload (ESP), the second electronic message is based on IPsec tunnel mode and IPsec

4   ESP, and the hash algorithm is a Message Digest 5 one-way hash function.

1   32.   (Currently Amended) A computer-readable medium carrying one or more sequences

2   of instructions for facilitating Internet security protocol (IPsec) based communications

3   through a device that employs address translation in a telecommunications network,

4   which instructions, when executed by one or more processors, cause the one or more

5   processors to carry out the steps of:

6   receiving a first electronic message from a first node, wherein:

7   the first node is associated with a first address;

8   the first electronic message is based on IPsec; ~~and~~

9   the first electronic message is associated with a first identifier;

10   the first identifier is generated by the first node; and

11   the first electronic message is addressed to a second network address;

12   the device generating a value based on the first identifier and a specified scheme;

13   sending the first electronic message to a second node base on the second network

14   address, wherein the first electronic message includes a particular network

15   address that is associated with the device instead of the first network address;

16   receiving a second electronic message from the second node, wherein:

17   the second electronic message is based on IPsec; ~~and~~

18   the second electronic message is associated with a second identifier that is

19   different than the first identifier[[,]] ~~wherein~~

20   the second identifier is generated, based on the first identifier and the specified

21   scheme, by the second node;

22   the device determining whether the second electronic message is directed to the first

23   node based on the value and the second identifier; and

24   sending the second electronic message to the first node at the first network address

25   when the second electronic message is determined to be directed to the first

26   node.

1   33.   (Currently Amended) ~~A~~ An apparatus for ~~computer-readable medium carrying one or~~

2   ~~more sequences of instructions~~ for facilitating Internet security protocol (IPsec) based

3   communications ~~through a device that employs~~ while employing address translation

4   in a telecommunications network, ~~which instructions, when executed by one or more~~

5   ~~processors, cause the one or more processors to carry out the steps of~~ comprising:

6   a processor; and

7   one or more stored sequences of instructions which, when executed by the processor,

8   cause the processor to carry out the steps of:

9   receiving a first electronic message from a first node, wherein:

10   the first node is associated with a first network address;

11   the first electronic message is based on IPsec; ~~and~~

12   the first electronic message is associated with a first identifier[[,]] ~~wherein~~

13   the first identifier is generated by the first node based on a second identifier

14   and a specified scheme; ~~and~~

15   the first identifier is different than the second identifier; and

16   the first electronic message is addressed to a second network address;

17   sending the first electronic message to a second node based on the second network

18   address, wherein the first electronic message includes a particular network

19   address that is associated with the apparatus instead of the first network

20   address;

21   receiving a second electronic message from the second node, wherein:

22   the second electronic message is based on IPsec; ~~and~~

23   the second electronic message is address to the particular network address;

24   the second electronic message is associated with the second identifier; and

25   the second identifier is generated by the second node;

26   generating a value based on the second identifier and the specified scheme;

27   determining whether the second electronic message is directed to the first node based

28   on the value and the first identifier; and

29   sending the second electronic message to the first node at the first network address

30   when the second electronic message is determined to be directed to the first

31   node.

1   34.   (Cancelled)

1   35.   (New) An apparatus for facilitating Internet security protocol (IPsec) based

2   communications while employing address translation in a telecommunications

3   network, the apparatus comprising:

4   means for receiving a first electronic message from a first node, wherein:

5   the first node is associated with a first network address;

6   the first electronic message is based on IPsec;

7   the first electronic message is associated with a first identifier;

8   the first identifier is generated by the first node; and

9   the first electronic message is addressed to a second network address;

10   means for generating a value based on the first identifier and a specified scheme;

11   means for sending the first electronic message to a second node based on the second

12   network address, wherein the first electronic message includes a particular

13   network address that is associated with the apparatus instead of the first

14   network address;

15   means for receiving a second electronic message from the second node, wherein:

16   the second electronic message is based on IPsec;

17   the second electronic message is addressed to the particular network address;

18	the second electronic message is associated with a second identifier that is
19	different than the first identifier; and
20	the second identifier is generated, based on the first identifier and the specified
21	scheme, by the second node;
22	means for determining whether the second electronic message is directed to the first
23	node based on the value and the second identifier; and
24	means for sending the second electronic message to the first node at the first network
25	address when the second electronic message is determined to be directed to
26	the first node.

1	36.	(New) An apparatus as recited in claim 35, further comprising:
2		means for receiving a third electronic message from a third node, wherein:
3		the third node is associated with a third network address;
4		the third electronic message is based on IPsec;
5		the third electronic message is associated with a third identifier;
6		the third identifier is generated by the third node; and
7		the third electronic message is addressed to the second network address;
8		means for generating an additional value based on the third identifier and the
9		specified scheme;
10		means for sending the third electronic message to the second node based on the
11		second network address, wherein the first electronic message includes the
12		particular network address that is associated with the apparatus instead of the
13		third network address;
14		means for receiving, after sending the first electronic message and the third electronic
15		message to the second node, the second electronic message from the second
16		node;
17		wherein:
18		the second electronic message is based on IPsec;
19		the second electronic message is addressed to the third network address;
20		the second electronic message is associated with the second identifier that is
21		different than the first identifier and the third identifier; and

22   the second identifier is generated, based on the third identifier and the

23   specified scheme, by the second node;

24   means for determining whether the second electronic message is directed to the third

25   node based on the additional value and the second identifier; and

26   means for sending the second electronic message to the third node at the third

27   network address, when the second electronic message is determined to be

28   directed to the third node.

1   37.   (New) An apparatus as recited in claim 35, wherein the specified scheme is selected

2   from the group consisting of a first scheme that produces a fixed length output, a

3   second scheme that includes a hash algorithm, and a third scheme that includes a

4   Message Digest 39 one-way hash function.

1   38.   (New) An apparatus as recited in claim 35, wherein:

2   the value is a hash value;

3   the second identifier is based at least in part on the hash value;

4   the hash value is comprised of a first plurality of bytes;

5   the second identifier is comprised of a second plurality of bytes;

6   a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first

7   plurality of bytes; and

8   the means for determining whether the second electronic message is directed to the

9   first node further comprises:

10   means for comparing the last pair of bytes of the second identifier to the first

11   pair of bytes of the hash value; and

12   means for determining that the second electronic message is directed to the

13   first node, when the last pair of bytes of the second identifier match the

14   firs pair of bytes of the hash value.

1   39.   (New) An apparatus as recited in claim 35, wherein:

2   the first node is an IPsec originator node;

3   the second node is an IPsec responder node;

4   the first identifier is a first IPsec security parameter index;

5   the second identifier is a second IPsec security parameter index;

6   the apparatus employs a feature selected from the group consisting of network address

7   translation (NAT), dynamic address NAT, and network address port translation

8   (NAPT);

9   and the apparatus further comprises:

10   means for creating and storing a mapping between the value and the first IPsec

11   security parameter index;

12   means for creating an association between the value and the first identifier; and

13   means for storing the association in a translation table.

1 40. (New) An apparatus as recited in claim 35, wherein the first electronic message and

2   the second electronic message are both based on an IPsec feature selected from the

3   group consisting of IPsec tunnel mode and IPsec Encapsulation Security Payload.

1 41. (New) An apparatus as recited in claim 35, further comprising:

2   means for creating an association between the first network address and the second

3   identifier, when the second electronic message is determined to be directed to

4   the first node;

5   means for storing the association in a table;

6   means for receiving a third electronic message from the second node, wherein the

7   third electronic message is based on IPsec and is associated with the second

8   identifier; and

9   means for determining that the third electronic message is directed to the first node

10   based on the association.

1 42. (New) An apparatus as recited in claim 35, further comprising:

2   means for receiving a third electronic from the second node, wherein:

3   the third electronic message is based on IPsec;

4   the third electronic message is addressed to the specified network address;

5   the third electronic message is associated with a third identifier that is

6   different than both the first identifier and the second identifier;

7   the third identifier is generated, based on the first identifier and the specified

8   scheme, by the second node;

9   means for determining whether the third electronic message is directed to the first

10   node based on the value and the third identifier; and

11   means for sending the third electronic message to the first node at the first network

12   address, when the third electronic message is determined to be directed to the

13   first node.

1   43.   (New) An apparatus as recited in claim 35, wherein the value is generated before the

2   second electronic message is received.

1   44.   (New) An apparatus as recited in claim 35, wherein the value is generated after the

2   second electronic message is received.

1   45.   (New) An apparatus for facilitating Internet security protocol (IPsec) based

2   communications while employing address translation in a telecommunications

3   network, comprising:

4   a processor; and

5   one or more stored sequences of instructions which, when executed by the processor,

6   cause the processor to carry out the steps of:

7   receiving a first electronic message from a first node, wherein:

8   the first node is associated with a first network address;

9   the first electronic message is based on IPsec;

10   the first electronic message is associated with a first identifier;

11   the first identifier is generated by the first node; and

12   the first electronic message is addressed to a second network address;

13   generating a value based on the first identifier and a specified scheme;

14   sending the first electronic message to a second node based on the second network

15   address, wherein the first electronic message includes a particular network

16   address that is associated with the apparatus instead of the first network

17   address;

18   receiving a second electronic message from the second node, wherein:

17

19   the second electronic message is based on IPsec;

20   the second electronic message is addressed to the particular network address;

21   the second electronic message is associated with a second identifier that is

22   different than the first identifier; and

23   the second identifier is generated, based on the first identifier and the specified

24   scheme, by the second node;

25   determining whether the second electronic message is directed to the first node based

26   on the value and the second identifier; and

27   sending the second electronic message to the first node at the first network address

28   when the second electronic message is determined to be directed to the first

29   node.

1   46.   (New) An apparatus as recited in claim 45, further comprising one or more stored

2   instructions which, when executed by the processor, cause the processor to carry out

3   the steps of:

4   receiving a third electronic message from a third node, wherein:

5   the third node is associated with a third network address;

6   the third electronic message is based on IPsec;

7   the third electronic message is associated with a third identifier;

8   the third identifier is generated by the third node; and

9   the third electronic message is addressed to the second network address;

10   generating an additional value based on the third identifier and the specified scheme;

11   sending the third electronic message to the second node based on the second network

12   address, wherein the first electronic message includes the particular network

13   address that is associated with the apparatus instead of the third network

14   address;

15   receiving, after sending the first electronic message and the third electronic message

16   to the second node, the second electronic message from the second node;

17   wherein:

18   the second electronic message is based on IPsec;

19   the second electronic message is addressed to the third network address;

20   the second electronic message is associated with the second identifier that is

21   different than the first identifier and the third identifier; and

22   the second identifier is generated, based on the third identifier and the

23   specified scheme, by the second node;

24   determining whether the second electronic message is directed to the third node based

25   on the additional value and the second identifier; and

26   when the second electronic message is determined to be directed to the third node,

27   sending the second electronic message to the third node at the third network

28   address.

1   47.   (New) An apparatus as recited in claim 45, wherein the specified scheme is selected

2   from the group consisting of a first scheme that produces a fixed length output, a

3   second scheme that includes a hash algorithm, and a third scheme that includes a

4   Message Digest 49 one-way hash function.

1   48.   (New) An apparatus as recited in claim 45, wherein:

2   the value is a hash value;

3   the second identifier is based at least in part on the hash value;

4   the hash value is comprised of a first plurality of bytes;

5   the second identifier is comprised of a second plurality of bytes;

6   a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first

7   plurality of bytes; and

8   the instructions for determining whether the second electronic message is directed to

9   the first node further comprises one or more stored instructions which, when

10   executed by the processor, cause the processor to carry out the steps of:

11   comparing the last pair of bytes of the second identifier to the first pair of

12   bytes of the hash value; and

13   when the last pair of bytes of the second identifier match the firs pair of bytes

14   of the hash value, determining that the second electronic message is

15   directed to the first node.

1 49. (New) An apparatus as recited in claim 45, wherein:

2 the first node is an IPsec originator node;

3 the second node is an IPsec responder node;

4 the first identifier is a first IPsec security parameter index;

5 the second identifier is a second IPsec security parameter index;

6 the apparatus employs a feature selected from the group consisting of network address

7 translation (NAT), dynamic address NAT, and network address port

8 translation (NAPT);

9 and the apparatus further comprises one or more stored instructions which, when

10 executed by the processor, cause the processor to carry out the steps of:

11 creating and storing a mapping between the value and the first IPsec security

12 parameter index;

13 creating an association between the value and the first identifier; and

14 storing the association in a translation table.

1 50. (New) An apparatus as recited in claim 45, wherein the first electronic message and

2 the second electronic message are both based on an IPsec feature selected from the

3 group consisting of IPsec tunnel mode and IPsec Encapsulation Security Payload.

1 51. (New) An apparatus as recited in claim 45, further comprising one or more stored

2 instructions which, when executed by the processor, cause the processor to carry out

3 the steps of:

4 when the second electronic message is determined to be directed to the first node,

5 creating an association between the first network address and the second

6 identifier;

7 storing the association in a table;

8 receiving a third electronic message from the second node, wherein the third

9 electronic message is based on IPsec and is associated with the second

10 identifier; and

11 determining that the third electronic message is directed to the first node based on the

12 association.

1   52.   (New) An apparatus as recited in claim 45, further comprising one or more stored

2   instructions which, when executed by the processor, cause the processor to carry out

3   the steps of:

4   receiving a third electronic from the second node, wherein:

5   the third electronic message is based on IPsec;

6   the third electronic message is addressed to the specified network address;

7   the third electronic message is associated with a third identifier that is

8   different than both the first identifier and the second identifier;

9   the third identifier is generated, based on the first identifier and the specified

10   scheme, by the second node;

11   determining whether the third electronic message is directed to the first node based on

12   the value and the third identifier; and

13   when the third electronic message is determined to be directed to the first node,

14   sending the third electronic message to the first node at the first network

15   address.

1   53.   (New) An apparatus as recited in claim 45, wherein the value is generated before the

2   second electronic message is received.

1   54.   (New) An apparatus as recited in claim 45, wherein the value is generated after the

2   second electronic message is received.

Docket No. 50325-0616 (Seq.No. 4621)